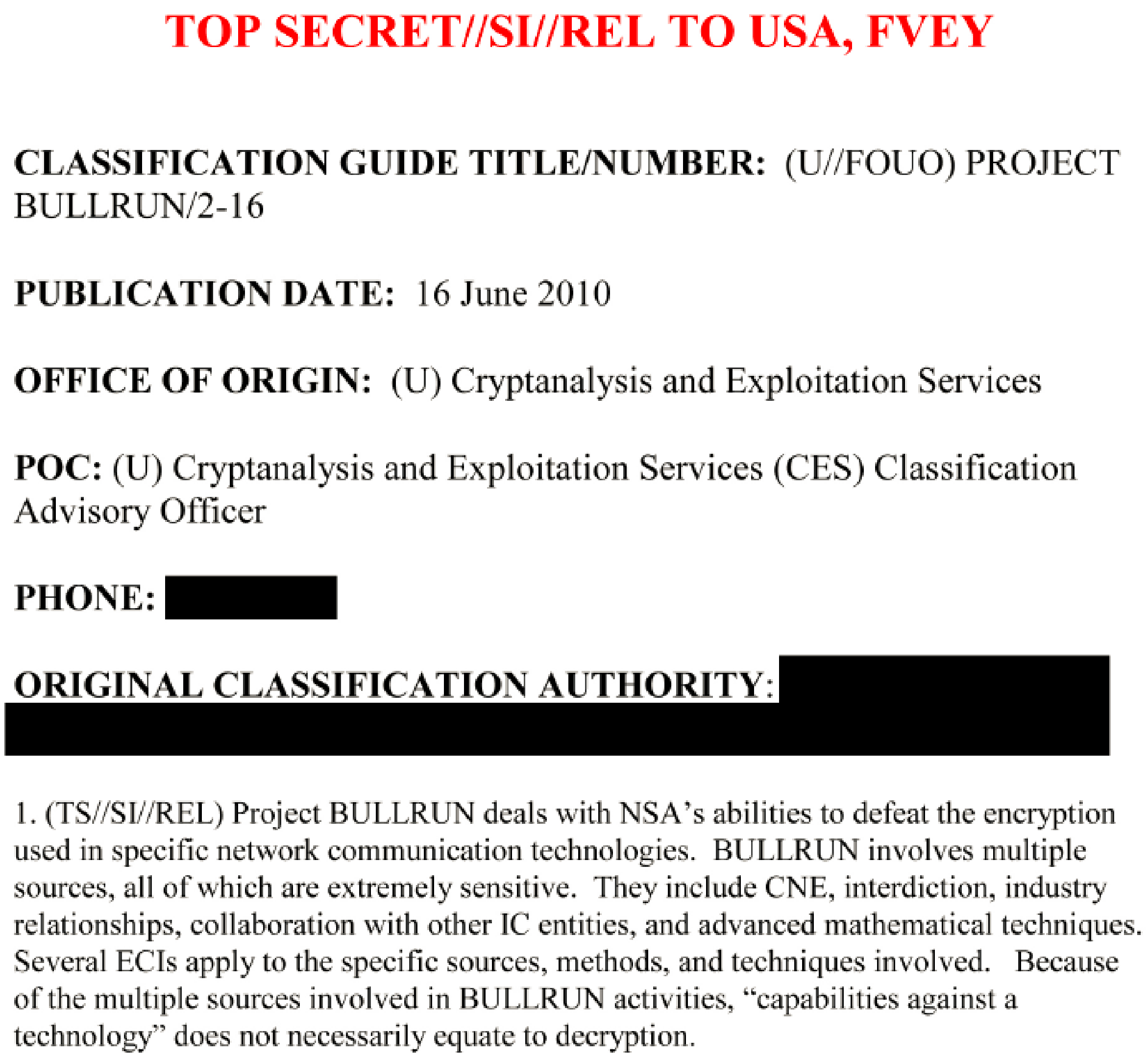
Info 206: Computing

Lecture 7

Cryptology

September 24, 2015

How did NSA break SSL?



TOP SECRET//SI//REL TO USA, FVEY

CLASSIFICATION GUIDE TITLE/NUMBER: (U//FOUO) PROJECT BULLRUN/2-16

PUBLICATION DATE: 16 June 2010

OFFICE OF ORIGIN: (U) Cryptanalysis and Exploitation Services

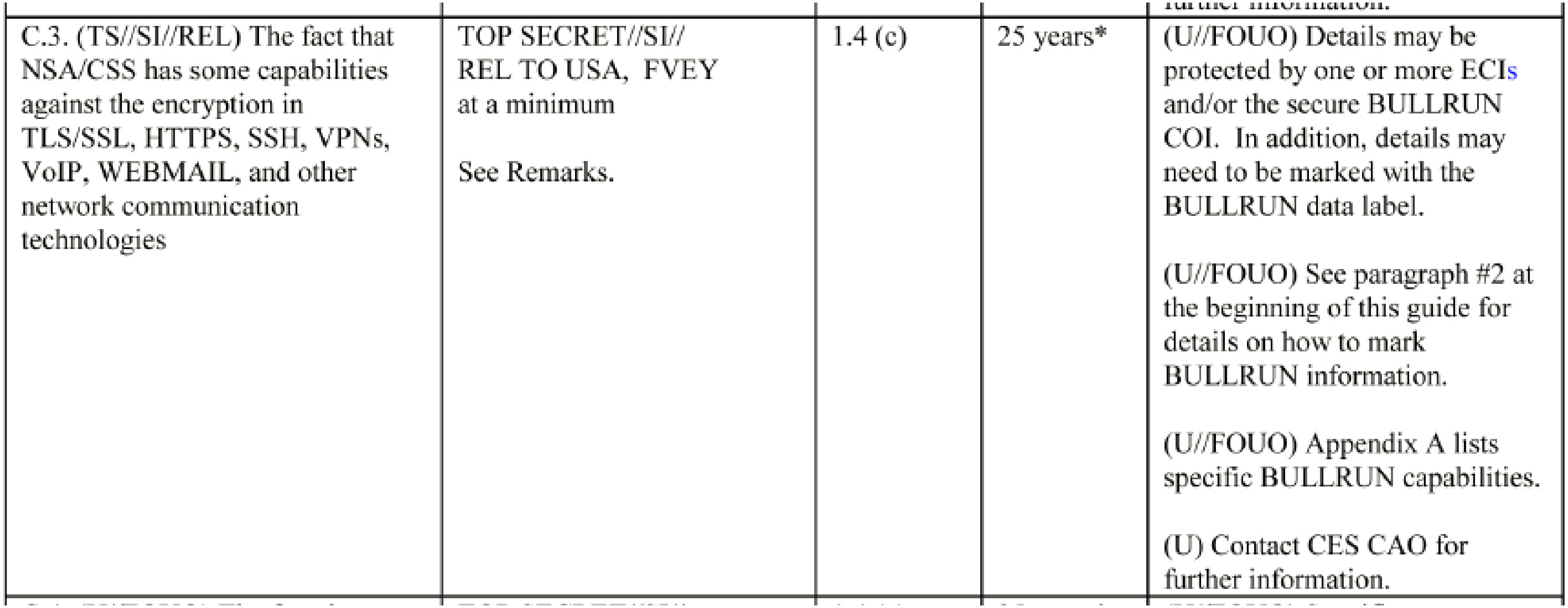
POC: (U) Cryptanalysis and Exploitation Services (CES) Classification Advisory Officer

PHONE: [redacted]

ORIGINAL CLASSIFICATION AUTHORITY: [redacted]

1. (TS//SI//REL) Project BULLRUN deals with NSA's abilities to defeat the encryption used in specific network communication technologies. BULLRUN involves multiple sources, all of which are extremely sensitive. They include CNE, interdiction, industry relationships, collaboration with other IC entities, and advanced mathematical techniques. Several ECIs apply to the specific sources, methods, and techniques involved. Because of the multiple sources involved in BULLRUN activities, "capabilities against a technology" does not necessarily equate to decryption.

How did NSA break SSL?



				further information.
C.3. (TS//SI//REL) The fact that NSA/CSS has some capabilities against the encryption in TLS/SSL, HTTPS, SSH, VPNs, VoIP, WEBMAIL, and other network communication technologies	TOP SECRET//SI// REL TO USA, FVEY at a minimum See Remarks.	1.4 (c)	25 years*	(U//FOUO) Details may be protected by one or more ECIs and/or the secure BULLRUN COI. In addition, details may need to be marked with the BULLRUN data label. (U//FOUO) See paragraph #2 at the beginning of this guide for details on how to mark BULLRUN information. (U//FOUO) Appendix A lists specific BULLRUN capabilities. (U) Contact CES CAO for further information.

- “Those not already briefed were gobsmacked”
- We will see how NSA broke SSL in next two lectures

Cryptology

- Cryptology = science of secret messages
- Subareas:
- Cryptography
  - Science of creating secret messages
- Cryptanalysis
  - Science of attacks on cryptography
- Traffic analysis
  - Science of studying patterns of messages

Example: Skype

- Skype encrypts messages
  - Cryptography
- An eavesdropper may intercept packets and attempt to decrypt them
  - Cryptanalysis
- Try to observe message patterns and find out who is communicating
  - Traffic analysis

Model of Cryptography

- Encryption

  $ciphertext \leftarrow Encryption(plaintext, key_{Encryption})$

- Decryption

  $plaintext \leftarrow Decryption(ciphertext, key_{Decryption})$

- Symmetric cryptography
  - $key_{Encryption} = key_{Decryption}$
- Asymmetric cryptography
  - $key_{Encryption} \neq key_{Decryption}$

Symmetric vs asymmetric crypto

- Symmetric cryptography
  - $key_{Encryption} = key_{Decryption}$
  - “Private key cryptography”

- Asymmetric cryptography
  - $key_{Encryption} \neq key_{Decryption}$
  - “Public key cryptography”

Cryptographic protocols

- A cryptographic protocol is a template for exchanging messages
- An important protocol is SSL/TLS
    - Secure socket layer
    - Transport layer security
- We will discuss this protocol next week

History of cryptography

- Goes back to Julius Caesar
  - Suetonius writes about Caesar’s invention of the Caesar cipher.
- World War I
  - Zimmerman telegraph
  - Black Chamber
- World War II
  - Japanese “Purple” cipher & Midway
  - German “Enigma” cipher & D-Day
  - NSA

Caesar cipher

- Each letter replaced by substitute
- Example key = -1
  - A → Z
  - B → A
  - C → B
  - …
  - Z → Y
- What does “HAL” (in *2001: A Space Odyssey*) become?

Caesar cipher

- How many keys are possible in a Caesar cipher?
- 26
  - Notice that key +27 = key +1
  - Keyspace
- The key +0 is a poor choice for a key
  - Weak keys
- Brute force attack
  - Try all possible keys

Notation

- $E()$ refers to the encryption function
  - e refers to an encryption
- $D()$ refers to the decryption function
  - d refers to a decryption
- K and k refer to keys
  - K_e is thus an encryption key
- m refers to a plaintext message
  - Or a message converted to a bit string or number
- c refers to a ciphertext message
  - Or a message converted to a bit string or number

Notation

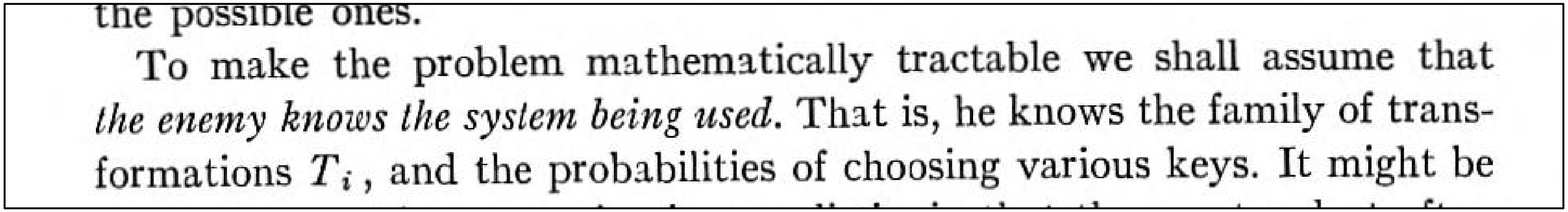
- Sometimes instead of writing $E(m, k)$ or $D(c, k)$ I will write $[m]_k$ or $[c]_k$

- You may see some people use the notation $E_k(m)$ and $D_k(c)$

- For symmetric ciphers only instead of writing $D(c, k)$ I may write $E^{-1}(c, k)$
    - Self-check: why only for symmetric ciphers?

“The enemy knows the system”

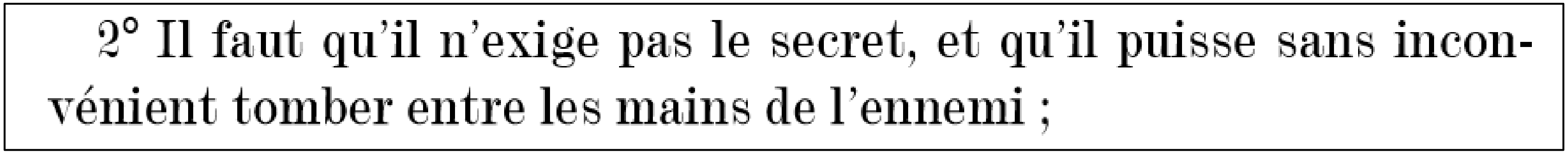
- (Claude) Shannon’s Maxim
  - “The enemy knows the system”



the possible ones.

To make the problem mathematically tractable we shall assume that *the enemy knows the system being used*. That is, he knows the family of transformations T_i, and the probabilities of choosing various keys. It might be

- (Auguste) Kerckhoff’s Principle
  - “[A cipher] should not require secrecy, and it should not be a problem if it falls into enemy hands”



2° Il faut qu’il n’exige pas le secret, et qu’il puisse sans inconvénient tomber entre les mains de l’ennemi ;

Security through obscurity

- Not required to publish the details of security
- But cannot depend on security of obscurity

- In cryptography, what is secret is keys

Brute force attacks

- We can try all possible keys
- We can usually recognize valid plaintext

- NGGNPXNGQNJA vs ATTACKATDAWN
- Unicity distance
  - Minimum number of characters of ciphertext needed for a single intelligible plaintext

Exclusive OR

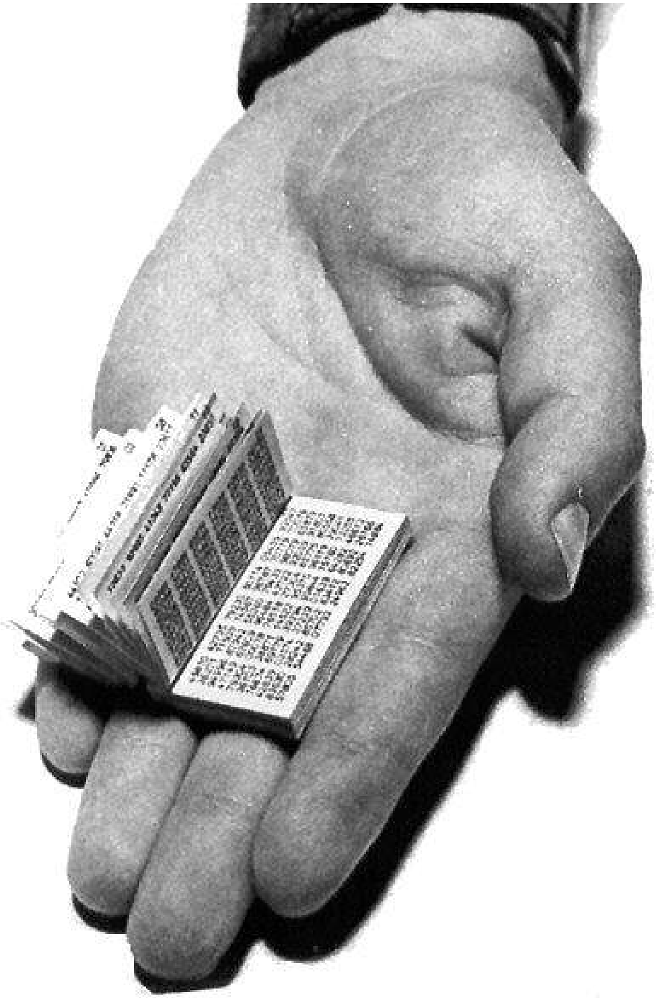
- Exclusive or is a binary operation
    - $0\ xor\ 0 = 0$
    - $0\ xor\ 1 = 1$
    - $1\ xor\ 0 = 1$
    - $1\ xor\ 1 = 0$
- If more than one digit, apply to each column independently
    - $0011\ xor\ 0101 = 0110$

One time pad

- Key: a list of truly random bits
- Both Alice & Bob have this key
- $E(m) = m\ xor\ k \qquad D(c) = c\ xor\ k$
- Can only use key once
- Perfectly secure, because unicity distance ∞

$$m = 10101010101010101010$$
$$k\ = 00110000000101100100$$
$$c\ = 10011010101111001110$$

One time pad



One time pad

- One time pad is perfectly secure
- But key size makes it impractical for use

DES - Data Encryption Standard (1977)

- Works on 64 bit block with 56 bit keys
- Developed by IBM (Lucifer) improved by NSA
- Brute force attack feasible in 1997

AES – Advanced Encryption Standard (1997)

- Rijndael cipher
  - Joan Daemen & Vincent Rijmen
- Block size 128 bits
- Key can be 128, 192, or 256 bits